Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 16 April 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- Fox News reports early 10,000 blank French passports were stolen in February, leading the FBI to warn U.S. law enforcement agencies to be on the lookout. (See item 8)
- The Associated Press reports the U.S. government on Thursday broadened a warning to airline passengers about possible measles exposure, adding three flights to a list of planes carrying infected Chinese babies who had just been adopted by U.S. parents. (See item 22)
- The Associated Press reports the U.S. State Department is considering a withdrawal of nonessential U.S. diplomats and family members from Saudi Arabia because of "credible indications of terrorist threats" aimed at Americans in that country. (See item 32)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *April 15, Mercury News (CA)* — **Record energy demand predicted. California state power officials warn that a record demand for electricity is expected this summer, which could leave California with limited power reserves and require businesses and residents to conserve energy.** The situation "is an important wake−up call," said Jan Smutny−Jones, executive director of the Independent Energy Producers, a trade association for energy sellers.

"It isn't time to hit the panic button but supplies are very tight." The concerns stem from a forecast prepared by the California Independent System Operator (ISO), which manages the state's power grid. **The forecast predicts a new all−time high peak demand at the same time that power available will be 873 megawatts less than was available last summer.** In a best case scenario −− with no natural disasters, transmission outages or national catastrophes −− the ISO expects the state's power supply to meet the anticipated peak demand in August. That's when demand is anticipated to be about 44,422 megawatts, but it would leave only 1,176 megawatts of power in reserve for any variation in demand that might arise, according to the draft report.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/8436212.htm?1c

[Return to top]

Chemical Sector

2. *April 14, NWO Netherlands Organization for Scientific Research* — **Batch control makes chemical reactions easier to manage. Two Dutch researchers have developed a method for managing batch productions. During a batch production, substances react in a reactor vessel according to a certain recipe to produce an end product. After the reaction the reactor is emptied and a new reaction with the same recipe is started. Chemist Eric van Sprang and chemical engineer Henk−Jan Ramaker have developed a control method that also takes the relationship between various process parameters into account.** The current methods of process control monitor all of the parameters during the reaction, such as pressure and temperature, separately. As a result of this the control process costs a lot of time and not all of the process disruptions are clearly visible. Batch control is important for safety, the environment and product quality. The quality of the product made in a batch process depends on the various parameters involved in the chemical reaction. However, these parameters are never the same for all batches. The researchers made a model to predict how large the variations can be without endangering the quality of the product. They first of all collected the process parameters from more than thirty batches and then described the process variation with the help of a model. Finally, they used this model to make two control cards that an operator can use to control the process.
Source: http://www.innovations−report.com/html/reports/life_sciences /report−28053.html

[Return to top]

Defense Industrial Base Sector

3. *April 15, Government Computer News* — **Department of Defense sets up group to test biometrics. The Department of Defense (DoD) announced Thursday, April 15, the formation of the Test and Evaluation Biometric Working Group to push best practices for biometric testing and evaluation.** DoD's Biometric Fusion Center said the working group is composed of various Defense agency personnel and members of each of the armed services. "The Biometrics Fusion Center is proud to support national security and global war on terrorism," said Sam Cava, director of the center. "We're working hard to provide the DoD

warfighter community with reliable, responsive and timely information on biometric technologies. To do this, we must work with all of the relevant stakeholders to develop state−of−the−art testing methodologies." The mission of the new working group includes coordinating test and evaluation activities and aligning processes and procedures.
Source: http://www.gcn.com/vol1_no1/daily−updates/25586−1.html

4. *April 15, BBC News (UK)* — **U.S. troops to stay longer in Iraq. Some 20,000 U.S. troops now serving in Iraq will have their tour of duty extended, Secretary of Defense Donald Rumsfeld has announced.** Rumsfeld said they would spend another 90 days in Iraq beyond their original one−year deployment. "The country is at war and we need to do what is necessary to succeed," he told a news conference. Rumsfeld said the extension came in response to a request by the commander of U.S. forces in Iraq, General John Abizaid.
Source: http://news.bbc.co.uk/2/hi/middle_east/3630433.stm

[Return to top]

Banking and Finance Sector

5. *April 15, CTV.ca* — **British Columbia police break up money laundering ring. Police in British Columbia, Canada, say they have broken up an operation that laundered the profits from the sale of Canadian marijuana to the United States.** The Vancouver−based outfit that handled more than $3 million a week from sales was raided by the Royal Canadian Mounted Police (RCMP). The police confiscated over four million dollars and expensive jewelry. The operation took U.S. funds from marijuana brokers and converted it to Canadian funds so that it could be spent legally. **This conversion process can be difficult especially since new regulations require financial transactions over $10,000 to be declared. "They know the financial systems. They use them well," RCMP Inspector George Pemberton said.** Police say that the suspects who brokered the movement of marijuana have a vast and meticulously planned cartel. Illegal marijuana is a $5−billion a year business in British Columbia, with much of the sales targeted to U.S. consumers.
Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1081996591040_41/?hub=Canada

6. *April 15, Finextra Research* — **Security scares to drive PINs at point−of−sale.** Consumer awareness of identity theft and card security fears are set to drive the adoption of Personal Identification Numbers (PINs) at the point−of−sale, according to two separate research reports into payment trends in the UK and U.S. markets. In the UK, research from MasterCard forecasts a surge in plastic debit payments following the nationwide roll−out of chip and PIN at the check−out. **In the U.S. market, a separate study by Dove Consulting and the American Bankers Association suggests that PIN debit will overtake signature debit within the next five years as the cost of PIN pads fall and consumers switch to safer ways to pay.** Debit cards were used for 31% of payments in the U.S. in 2003, while cash and checks accounted for 47% of payments, compared to respective figures of 21% and 60% in 1999.
Source: http://www.finextra.com/topstory.asp?id=11631

7. *April 14, Computerworld* — **Visa and MasterCard roll out vulnerability assessment**

initiatives. Leading credit card providers MasterCard and Visa International are rolling out similar programs to help their merchants and members secure their online ventures. This June, high−volume merchants and payment processors that do business on the Web and want to work with MasterCard International will have to conduct quarterly vulnerability assessments of their Websites. "We believe the majority of events we read about with worms could be averted through vulnerability assessment," says John Verduschi, vice president of Ebusiness and Emerging Technologies at MasterCard, which has drawn up a list of a dozen approved network−based scanning services. With an estimated 7 per cent of all of MasterCard's $921.6 billion in annual card purchases now taking place on the Web, it is no wonder that the global payments company is making vulnerability assessment mandatory. "With the number of documented system vulnerabilities increasing each year, organizations need to take proactive measures that prevent the loss of valuable information and protect business productivity," said Joy Ghosh, Enterprise Sales director, Asean and India, Symantec. Source: http://www.computerworld.com.sg/pcwsg.nsf/unidlookup/57FCE49111433ED848256E7600194672?OpenDocument

[Return to top]

Transportation Sector

8. *April 15, Fox News* — **FBI warns of stolen French passports. Nearly 10,000 blank French passports were stolen in February, leading the FBI to warn U.S. law enforcement agencies to be on the lookout.** "These stolen passports are of particular concern because France participates in the Visa Waiver Program that allows visitors from 27 nations to enter the United States for pleasure for 90 days without a visa," the FBI said in the warning issued Wednesday, April 15. "Fraudulent or illicitly acquired travel documents, such as passports and visas, compromise the security of U.S. borders by providing means to gain unlawful entry into the country. Fraudulently issued or altered passports can be used by criminals, including terrorists, to adopt false identities, impersonate other citizens or conceal suspicious travel." French officials notified the U.S. Embassy in Paris that 6,300 blank passports were stolen on February 3 and another 3,000 disappeared on February 10, the bulletin said. **The February 3 incident, the FBI said, also included the theft of 5,000 blank French driver's licenses, 10,000 blank car ownership certificates, 25 titres de voyages (Geneva Convention travel documents) and 1,000 international driver's licenses without any identification numbers.** Source: http://www.foxnews.com/story/0,2933,117200,00.html

9. *April 15, New York Times* — **Test screening planned for trains at Maryland station. The Transportation Security Administration plans to begin testing techniques for improving passenger rail security at a station in New Carrollton, MD, that is served by Amtrak and commuter trains that run between Washington, D.C., and Baltimore, MD,** according to government officials. The agency will conduct passenger screening, but not the way it is done at airports. "It is not going to be as invasive as airport screening is," said Dan Stessel, a spokesperson for Amtrak. "No one at New Carrollton will be asked to remove their belt or shoes." **The new program, called the "Transit and Rail Inspection Pilot," or TRIP, will begin next month. Its focus is not guns or knives, but bombs, according to officials. Techniques could include bomb−sniffing dogs or electronic detectors,** they said. Government security officials say they have discussed whether to compare the names of

railroad ticket buyers to "watch lists," as is done with airplane passengers. Stessel said that Amtrak had the capacity to supply such names but had not been asked to do so.
Source: http://www.nytimes.com/2004/04/15/national/15CND−TRAI.html

10. *April 15, Associated Press* — **Wireless radios ready for Metrorail tunnels. Warning that public transit is a "prime target for terrorists," Washington, D.C. Mayor Anthony A. Williams on Wednesday, April 14, announced the expansion of a wireless network to the city's Metrorail tunnels.** Four years ago, D.C. firefighters' hand−held radios were not working as they tried to rescue trapped subway passengers during a tunnel fire. City officials said D.C.−area radios now have more reach than those in many other major metropolitan areas. The new underground system interfaces with the aboveground wireless network completed in September. **City officials said the underground network is being used by D.C. firefighters and emergency medical personnel.** The new system operates at the public safety industry standard level at which speech is understandable with only minor distortion, rarely requiring repetition of messages. Fire officials have said before the system changes, radios would work in tunnels only if one firefighter was close enough to see another, and the messages would not reach the surface.
Source: http://www.washtimes.com/metro/20040414−110317−4007r.htm

11. *April 15, New York Times* — **Airlines are looking at a long, hot summer. According to the Air Transport Association, each 1−cent increase in the price of fuel, now over $1 a gallon, costs the industry $180 million. The airline industry is beginning to see what was supposed to be a promising year slip away, because of rising fuel costs, brutal competition, and its own lingering financial headaches.** While no one is predicting this summer will be as bad operationally as the infamous summer of 2000, when one of four flights was delayed, canceled or diverted, there are fears that a difficult season lies ahead. "In the past, a good summer could have paved its way to a break−even year; this summer, it probably won't," said Darin Lee, senior managing economist with LECG, a consulting firm in Cambridge, MA. Some industry analysts say first−quarter losses could reach $1 billion or more for the carriers, even though traffic is rebounding to levels last seen before the September 2001 terrorist attacks. "There are a number of carriers that are teetering on the edge, and this is one those things that could put them into bankruptcy or extinction," said Jeffrey J. Misner, Continental Airline's chief financial officer.
Source: http://www.nytimes.com/2004/04/15/business/15air.html

12. *April 15, Associated Press* — **Jets fly near each other during blackout. Two commercial jets flew within 4.2 miles of each other at the same altitude during a power outage at the Los Angeles, CA, airport this week.** Federal standards require at least a 5−mile gap. The violation occurred because an air−traffic controller misjudged the turning rate of one plane and put it in a landing position too soon, FAA spokesperson Donn Walker said. Both planes were at 28,000 feet. Doug Church, spokesperson for the National Air Traffic Controllers Association, said **the power outage was to blame because controllers were swamped with work as a result.**
Source: http://seattlepi.nwsource.com/national/apus_story.asp?category=1110&slug=BRF%20Airport%20Blackout

[Return to top]

Postal and Shipping Sector

13. *April 15, Federal Communications Commission* — **FCC adopts rule changes for improved radio frequency identification systems. In an effort to increase homeland security and improve the efficiency of commercial shipping operations, the Federal Communications Commission on Thursday, April 15, adopted a Third Report and Order that allows for the operation of improved radio frequency identification (RFID) systems for use in conjunction with commercial shipping containers.** This action is expected to result in lower shipping costs and improved security at ports, rail yards and warehouses in commercial and industrial settings by enabling the contents of containers to be rapidly inventoried. These improvements will also help system users determine whether tampering with their contents has occurred during shipping. RFID systems use radio signals to identify items. Uses of RFID include electronic toll collection such as the E−Z Pass system and anti−theft tags. An RFID system consists of a tag mounted on the item to be identified and a device that receives information transmitted from the tag. The Order increases the maximum signal level permitted for RFID systems operating in the 433.5−434.5 MHz band to facilitate more reliable transmissions with greater range than the rules previously allowed.
    Source: http://www.fcc.gov/

[Return to top]

Agriculture Sector

14. *April 15, Oster Dow Jones Commodity News* — **Alfalfa pests spotted in Kansas. Alfalfa weevils are showing up in force in some central Kansas fields, according to Kansas State University entomologist Jeff Whitworth.** Whitworth, who examined several central Kansas alfalfa fields the first week in April, said that he found plenty of alfalfa weevil larvae, especially south of Interstate 70. **"About 80 percent were first instars (post embryo stage), which means eggs are probably still hatching and damage is noticeable only on the upper terminals of the plants,"** said Whitworth, who is a field crop specialist with K−State Research and Extension. Whitworth said he found one to eight larvae per stem with little feeding damage apparent so far. But, "as these larvae grow and more hatch, damage will become more visible," he said.
    Source: http://www.agprofessional.com/show_story.php?id=24571

[Return to top]

Food Sector

15. *April 15, Reuters* — **Japan official: Blanket mad cow tests to continue. Japan plans to keep testing all cattle for mad cow disease even though some Japanese experts say it is unnecessary, and Tokyo will continue asking the U.S. to do the same, a government official said on Thursday, April 15.** "We are carefully following discussions by experts," some of whom are calling for a review of Japan's blanket testing of all cattle for mad cow disease, Vice Agriculture Minister Mamoru Ishihara told a news conference. "On the issue of

U.S. beef imports, our position is that testing should match the measures taken in Japan where all domestic cattle is checked," Ishihara said. **Japan suspended U.S. beef imports after the United States discovered its first case of mad cow disease in late December last year, halting trade which amounted to nearly $1.4 billion in 2003.** Talks are at an impasse over Tokyo's demand, rejected by Washington, that all slaughtered cattle be tested for the brain wasting disease. Ishihara was responding to a question on the government's view after a panel of experts earlier in the day suggested that a review be made of Japan's policy of blanket testing.
Source: http://www.alertnet.org/thenews/newsdesk/T292064.htm

16. *April 15, Food Production Daily* — **Poultry poisoning breakthrough. Scientists from the Institute of Food Research (IFR), UK, have found that specific probiotics can destroy pathogenic bacteria living in the gut of poultry. The discovery could help remove the threat of bacterial food poisoning from the food chain.** The team screened thousands of non−pathogenic bacteria from adult chicken guts to identify strains that might have probiotic qualities. They found that Lactobacillus johnsonii cleared the pathogenic bacterium, Clostridium perfingens, from the gut of chicks. This bacteria can exist in the chicken gut without causing disease to the animal. However, it has also been known to produce toxins associated with necrotic enteritis. In humans, the symptoms of this condition are intense abdominal cramps and diarrhea, sometimes accompanied by vomiting. The probiotic also reduced colonisation of the small intestine of poultry by E. coli, but did not clear it completely. **This research has shown that specific probiotics can be used to target and eliminate a specific pathogen.**
Source: http://www.foodproductiondaily.com/news/news−NG.asp?id=51385

17. *April 14, Reuters* — **FDA warns feed plant. The Food and Drug Administration (FDA) said a Sanderson Farms Inc. (SAFM) plant produced adulterated animal feed and ordered the poultry company to immediately document how it would fix the problems. The FDA said the company's animal feed mill in Gallman, Mississippi, violated federal regulations for medicated feed.** "You should take prompt action to correct these violations, and you should establish a system whereby such violations do not recur," said the FDA letter, dated April 7. The FDA said it found "significant discrepancies" between actual drug usage in the plant's chicken feed and the usage that was recorded. The agency warned the company that corrective measures must be taken within 30 days or it would face regulatory action, which could include suspension of operations. Mississippi−based Sanderson Farms said in a statement that the FDA request grew out of a routine January inspection of its Gallman feed mill, and that Sanderson Farms provided the agency with documentation of its corrective actions on April 9.
Source: http://money.iwon.com/jsp/nw/nwdt_rt.jsp?cat=USMARKET&src=201&feed=reu&section=news&news_id=reu−n14424980−u2&date=20040414&alias=/alias/money/cm/nw

[Return to top]

Water Sector

18. *April 15, Associated Press* — **Denver imposes tough water restrictions. For the third straight year, millions of Coloradans will face water−use restrictions as utilities parcel out**

supplies from another season of disappointing snowfall. Denver Water, which serves 1.2 million customers in Denver and some of its burgeoning suburbs, was the latest to crack down. Directors of the utility voted Wednesday, April 14, to approve restrictions, two days after Aurora's City Council did the same thing. After May 1, Denver Water's residential customers will be allowed to water only twice a week, for 15 minutes per zone. There will be a surcharge for heavy water users and increased fees for new connections to the water system. First−time violators will get a warning. Fines for subsequent violations start at $250 and could rise to $1,000.
Source: http://www.sltrib.com/2004/Apr/04152004/utah/157221.asp

[Return to top]

Public Health Sector

19. *April 15, Washington Post* — **Government considers new smallpox vaccine. Buoyed by promising results in animal experiments, government officials are contemplating buying massive quantities of a new type of smallpox vaccine to supplement the national stockpile already assembled in the aftermath of the September 11, 2001, attacks.** Scientists believe that unlike any of the vaccines now available, the new vaccine may be effective in protecting against the deadly infectious disease without the risk of serious, and occasionally lethal, side effects. Efforts to develop the new vaccine, underway for several years, have taken on an air of urgency after safety concerns stalled a 2003 campaign to vaccinate millions of health care and emergency workers who might be first to respond to a biological attack. As doubts grow about the existing vaccines, scientists are increasingly optimistic about the prospects for the experimental vaccine, called Modified Vaccinia Ankara (MVA). Scientists say recently conducted studies using MVA on mice and monkeys indicated the vaccine is both effective and safe, results that are especially encouraging for the some 30 percent of the population that is not supposed to take any of the vaccines now available because of a high risk of complications.
Source: http://www.washingtonpost.com/wp−dyn/articles/A13095−2004Apr 14.html

20. *April 15, Associated Press* — **Flu shot makers say orders filling up fast for next season. Overwhelming demand for flu shots last season is causing this year's vaccine orders to fill up fast. So much so that there might not be as many extra doses left for sale during the upcoming season.** "We believe there may be less in−season doses available," said Philip Hosbach, vice president for new products and immunization policy for Aventis Pasteur, which provides half of the U.S. flu shot supply from its plant in Swiftwater, PA. Even though the start of the next flu season is still half a year away, health agencies and hospitals are already placing their orders because the vaccine takes months to manufacture. Production is somewhat limited and if vaccine makers receive many pre−orders, fewer shots will be available for sale during the season. In addition, the U.S. Centers for Disease Control and Prevention is wanting to create for the first time a massive flu shot stockpile to avert shortages like those experienced last winter.
Source: http://www.accessnorthga.com/news/ap_newfullstory.asp?ID=361 10

21. *April 15, Infectious Diseases Society of America* — **Military personnel accidentally vaccinated against smallpox. Ten U.S. military personnel were discovered to be HIV−positive after being vaccinated against smallpox, but did not experience any harmful effects from the vaccination.** In people with weakened immune systems, there is a chance that

the live virus in the smallpox vaccine, rather than immunizing them, can result in an infection that gets progressively worse. People who are known to be HIV−positive would not typically be given a smallpox vaccination because of this potentially fatal risk. More than 438,000 U.S. soldiers were vaccinated against smallpox between December 2002 and October 2003. Of the 10 later identified as HIV−positive, only three were known to be "primary" vaccine recipients, or had never been vaccinated before. Those who had previously received smallpox vaccinations may have benefited from some "leftover" immunity, but the fact that none of the soldiers had full−blown AIDS at the time of vaccination was probably a key factor in preventing a dangerous reaction.
Source: http://www.eurekalert.org/pub_releases/2004−04/idso−hum04150 4.php

22. *April 15, Associated Press* — **CDC expands measles warning for travelers. The U.S. government on Thursday, April 15, broadened a warning to airline passengers about possible measles exposure, adding three flights to a list of planes carrying infected Chinese babies who had just been adopted by U.S. parents.** Passengers on those flights who develop fever or rash on or before Saturday, April 17, should see a doctor, the U.S. Centers for Disease Control and Prevention (CDC) said. **The warnings came after measles was confirmed in two more adopted Chinese babies recently flown to their new U.S. homes. Four cases were identified last week. Three more are suspected.** Of the six confirmed cases, there were four in Washington state and one each in Maryland and New York.
Source: http://seattlepi.nwsource.com/health/aphealth_story.asp?category=1500&slug=Measles%20Outbreak

23. *April 14, Voice of America* — **Polio reported in Botswana. The World Health Organization (WHO) says Botswana has reported its first case of polio in 13 years.** The UN health agency said Wednesday, April 14, that the virus that infected a seven−year−old boy in Botswana is genetically linked to a polio outbreak in Nigeria. **Botswana, declared polio−free in 1991, says it will conduct a national emergency immunization campaign because of the new case.** The WHO has blamed the northern Nigerian state of Kano for a resurgence of polio in the region. Islamic leaders in Kano have refused to allow UN agencies to immunize the population for polio. The current number of polio cases worldwide is just over 650, down from 350,000 about 15 years ago. Most new cases are in Nigeria. **And the WHO says polio is now appearing in nations where it had been eradicated.**
Source: http://www.voanews.com/article.cfm?objectID=48222927−6681−4EC1−A90F8CC38D8258A2

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24.

April 14, Government Computer News — **'Clock ticking' on interagency radio network.** The departments of Homeland Security, Justice and Treasury expect to solicit proposals soon for the Integrated Wireless Network (IWN) for federal law enforcement agencies. The program is underfunded and overdue, but agencies cannot afford to keep putting money into existing infrastructures, said Michael Duffy, deputy CIO for electronic government at Justice. Duffy outlined the program Wednesday, April 14, at a federal IT market conference in Falls Church, VA. **IWN will be implemented over five to 10 years under a performance−based contract developed from a statement of objectives**. The statement from the joint program office established by the three departments is expected to be finished in four or five weeks. An informational conference for potential vendors is scheduled for April 27. **IWN is being driven by the need to replace outdated equipment, establish interoperable communications—including data transfers—between agencies, and reduce the amount of radio frequency bandwidth consumed by federal law enforcement**. IWN will not serve state and local law enforcement agencies but will provide connectivity to them.
Source: http://www.gcn.com/vol1_no1/daily−updates/25577−1.html

[Return to top]

Information and Telecommunications Sector

25. *April 15, The Register* — **NetSky−V spreads on auto−pilot.** Yet another NetSky virus arrived on the scene Thursday, April 15. NetSky−V spreads using a well known Internet Explorer vulnerability, connected with the handling of XML pages. Instead of depending on users double clicking on infectious email attachments, the worm can spread automatically across vulnerable Windows boxes. **Users can be infected by NetSky−V simply by reading an infected email.** Most anti−virus firms rate NetSky−V as low−to−medium risk. **Emails contaminated by NetSky−V come with subject lines such as 'Converting message. Please wait...' and exploit code which attempts to download a copy of the worm from an infected user's computer.** The worm's payload contains code designed to spread infectious emails to addresses harvested from victim machines, which become zombie drones. From April 22−29, NetSky−V is programmed to launch a denial of service attack on file−sharing and warez websites.
Source: http://www.theregister.co.uk/2004/04/15/pesky_netsky/

26. *April 15, CNET News.com* — **FTC to shine light on spyware.** Pressure is growing for new rules to curtail malicious programs known as spyware, once again raising a vexing problem for the Internet age: Can software risks be regulated into submission? The issue will get a high−profile hearing Monday, April 19, when the Federal Trade Commission (FTC) plans to convene a workshop on the dangers of spyware. In a common scenario, such programs might bombard victims with unwanted ads or, more rarely, allow hackers to snoop on Web surfing activities and steal confidential data such as passwords to online bank accounts. **The hearing could be the first step toward federal action against spyware companies, following the path the FTC has previously taken on spam e−mail and other Internet privacy issues.** It also highlights rising national concern about this ill−defined category of computer pest. **The pitch of consumer complaints about spyware and adware now rivals that of the outcry against spam several years ago, and is prompting response from legislators in Congress and in a growing number of states.**
Source: http://news.com.com/2100−1024_3−5191822.html?tag=nefd.lede

27. *April 15, Federal Computer Week* — **Network Nebraska opens for business.** Nebraska officials this week formally launched a statewide telecommunications initiative that links government agencies, schools and colleges. Network Nebraska, a cooperative project that includes a number of different telecommunications companies, is aimed at offering affordable broadband Internet connections to all areas of the largely rural state. It also pushes the government's reach further out to these areas. **Network Nebraska is one of the first such state initiatives to use MultiProtocol Label Switching (MPLS), a technology that allows various types of network protocols such as Frame Relay, Asynchronous Transfer Mode, Ethernet and IP to be consolidated into a single infrastructure, reducing both capital and operational expenses**. It also enables voice, video and data traffic to be easily integrated onto this common backbone. Officials tout the new network as a major source of savings.
Source: http://fcw.com/geb/articles/2004/0412/web−nebr−04−15−04.asp

28. *April 15, Federal Computer Week* — **Vulnerability database opens.** A freely available, independent database aimed at logging all security vulnerabilities on the Internet, in development since 2002, has been formally opened for public use. **The Open Source Vulnerability Database (OSVDB) collects information mainly from mailing lists that discuss vulnerabilities and from submissions from other sources. Members of the OSVDB verify and catalog all reports that come to the group**. Each recognized flaw is given a unique identifier for inclusion in the database. The database currently has about 1,900 cataloged vulnerabilities, with some 2,700 submissions outstanding: ww.osvdb.org
Source: http://fcw.com/fcw/articles/2004/0412/web−osvdb−04−15−04.asp

29. *April 14, Techworld.com* — **HP servers holed twice.** Hewlett−Packard Co. (HP) has been hit by two security holes−−one in its Internet Express, used with Tru64 servers, and a second in its authentication system OpenView. **A number of serious vulnerabilities have been found in the Washington University FTP daemon (WU−FTPD)** which forms part of HP's Internet Express, its collection of internet and administration software provided with Tru64 AlphaServer systems. The most serious of these vulnerabilities affects versions up to 2.6.2 of the software, delivered as part of Internet Express 6.2, and is caused by a boundary error in the S/KEY challenge handling procedure. **It can be exploited by putting in over−long user details to create a buffer overflow. Then, a malicious program can be run on the computer.** For the vulnerabilities to be exploitable, S/KEY authentication must be enabled, reducing the overall risk. **HP also acknowledged a "moderately critical" vulnerability in OpenView Operations**, specifically in its authentication facility, affecting versions 7.x of OpenView for HP−UX and Solaris, as well as Version 6.x of OpenView VantagePoint for the same two OSes. In this case, the vulnerability consists of the possibility of bypassing the authentication process, caused by a missing authentication check.
Source: http://www.infoworld.com/article/04/04/14/HNhpholes_1.html

30. *April 13, eSecurity Planet* — **Maryland lawmakers pass anti−spam bill. Maryland lawmakers this week passed a bill aimed at "kingpin," or high−volume, spammers that would punish offenders, especially repeaters, with jail time, monetary fines and loss of personal property.** The bill has been sent to Governor Robert L. Ehrlich Jr. for his signature. **It allows state law enforcement agencies to seek criminal penalties including three to ten years in jail; fines from $5,000 to $25,000; and forfeiture of personal property**. Also, the

bill contains a provision which would enable authorities to get injunctions against spammers enjoining them from continuing to violate the law, effectively putting them out of business. Maryland State Delegate Neil Quinter and co−author State Senator Rob Garagiola said that local authorities might have greater motivation to go after a particular case, for example, if a local business were the victim. In fact, **while the federal law focuses on consumers, Quinter and Garagiola found that businesses are equally harmed. Dealing with spam costs money and lowers productivity; it can also hurt a company's image when spammers spoof the address of a legitimate business.**
Source: http://www.esecurityplanet.com/trends/article.php/3339971

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_NETSKY.P** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	80 (www), 135 (epmap), 21 (ftp), 53 (domain), 25 (smtp), 111 (sunrpc), 57 (priv−term), 113 (ident), 23 (telnet), 81 (hosts2−ns) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

31. *April 15, CNN* — **Europe: No deal with bin Laden. European politicians have ruled out negotiations with Osama bin Laden after a tape that the CIA says is likely to be the al Qaeda leader offered a truce to European nations if they pulled troops out of Muslim countries.** European Commission President Romano Prodi said there could be no negotiating under a "terrorist threat." **The CIA, after evaluating the tape, said Thursday, April 15, that although it was impossible to be absolutely sure the voice on the tape was bin Laden's, it most likely was.** In Britain, the Foreign Office said there was no proof the voice on the tape was bin Laden. However, the message was being taken seriously. Arab language TV network Al−Arabiya aired Wednesday, April 14, what it said was an audio tape from bin Laden, in which he threatened revenge on America, but offers a truce to European states.
Source: http://www.cnn.com/2004/WORLD/asiapcf/04/15/binladen.tape/in dex.html

32.

April 15, Associated Press — **Some U.S. diplomats may leave Saudi Arabia. The State Department is considering a withdrawal of nonessential U.S. diplomats and family members from Saudi Arabia because of "credible indications of terrorist threats" aimed at Americans in that country, it was announced Thursday, April 15.** The U.S. Embassy in Saudi Arabia, in a message sent Wednesday, April 14, to American citizens in the country said the U.S. government "continues to receive credible indications of terrorist threats aimed at American and Western interests in Saudi Arabia." The threats include the targeting of diplomatic and other official facilities and residential compounds in Riyadh, the message said. It noted that there have there have been a number of violent clashes between security forces and heavily armed militants in various neighborhoods in Riyadh.
Source: http://www.grandforks.com/mld/grandforks/news/world/8439045. htm

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP